Kódovanie, šifrovanie, digitalizácia, komprimácia

V živote sa stretávame s množstvom informácií, ktoré nie sme schopní zapamätať si. Preto ich určitým spôsobom kódujeme. Napr. adresa bydliska, EČV, čiarový kód tovaru, Morseova abeceda, Braillovo písmo. **Kódovanie používame vtedy, keď vyjadrovanie bežnými slovami by bolo zdĺhavé alebo náročné na miesto či čas.**

Kódovanie informácií:

- **prevod informácií do takej podoby, aby bol umožnený prenos informácií a aby ich prijímateľ pochopil (*Braillovo písmo* pre prenos informácie k nevidiacom),**
- **je proces, pri ktorom sa každému znaku alebo postupnosti znakov daného súboru znakov (vzorov) jednoznačne priradí znak alebo postupnosť znakov (obrazov) z iného súboru znakov,**
- transformácia určitej informácie z jednej formy na druhú pomocou určitého postupu - algoritmu, ktorý je väčšinou verejne známy.

Písmo – jedným z kódov, ktorého používanie si ani neuvedomujeme je písmo. Ten, kto nepozná jednotlivé písmena a nedokáže ich spojiť do slov rodného jazyka, ťažko pochopí zmysel vety.
Počítače pracujú iba s digitálnymi informáciami, preto potrebuje informácie, ktoré chceme spracovať pomocou počítača kódovať do **binárneho kódu**, teda do tvaru 0 a 1.

Digitalizácia

Digitalizácia je kódovanie údajov a informácií do číselnej podoby. Digitalizácia je prevod analógových informácií na digitálne. Ku každému údaju sa priradí určitý počet bitov čiže jedinečná kombinácia jednotiek a núl. Toto priradenie musí byť také, aby sa údaj z digitálnej podoby dal jednoznačne pretransformovať späť do analógového tvaru.

Binárny kód alebo dvojkový kód je kód, v ktorom súbor znakov cieľovej množiny zobrazenia pozostáva iba z dvoch rôznych znakov, napríklad z 0 a 1.

Podľa spôsobu získavania dát delíme digitalizáciu na:

- **Primárnu** – získanie digitálneho obrazu priamym zberom digitálnou kamerou, prípadne iným snímačom.
- **Sekundárnu** – získanie digitálneho obrazu digitalizovaním analógového obrazu spravidla skenerom.

Šifrovanie

Kódy veľmi často používajú vojaci, námorníci alebo policajti (kód 75 – naháňam zlodeja). **Pokiaľ je účelom kódovania aj určité utajenie informácií, hovoríme o šifrovaní.**

Kryptológia – veda zaoberajúca sa šiframi. Kryptológia pozostáva z **kryptografie**, ktorej cieľom je vytvoriť nerozlúštiteľnú šifru a **kryptoanalýzy**, ktorá ju má rozlúštiť.
Pokiaľ chceme údaje zašifrovať, potrebujeme na to minimálne šifrovací/dešifrovací **algoritmus** – postup, na základe ktorého sa pôvodná správa zmení na zašifrovanú. Väčšina

algoritmov vyžaduje na šifrovanie a dešifrovanie **kľúč**. Cieľom šifrovania vždy bolo nájdenie takej **šifry**, ktorú by nezasvätený nemohol rozlúštiť.

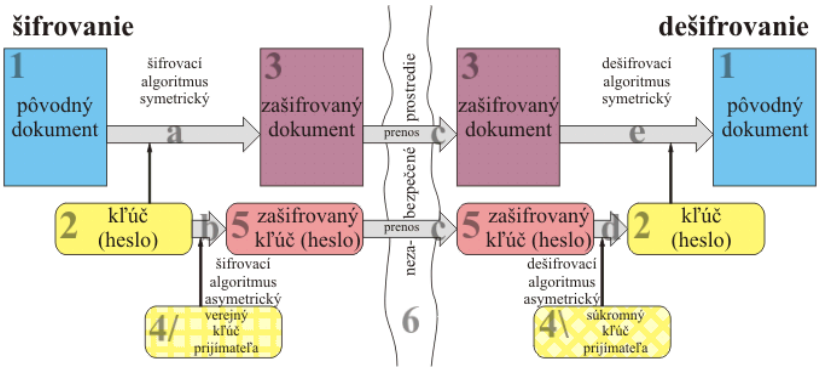
Šifry:

- Scytale – šifrovací valec,
- Cézarová šifra – spočíva v posúvaní znakov o zadanú hodnotu,
- Vigenerová šifra – posúva znaky, ale posun je daný zložitejším algoritmom,
- transpozičná šifra – napísanie textu do tabuľky tak, aby text tiekol odhora nadol.

Súčasné šifry možno rozdeliť do dvoch základných kategórií:

- **Symetrické šifry** predstavujú kategóriu šifier, v ktorých sú šifrovacie kľúče pre šifrovanie a dešifrovanie rovnaké.
- **Asymetrické šifry** sú založené na myšlienke používania dvojice kľúčov – verejného a súkromného. Prostredníctvom jedného z nich sa správa zašifruje, prostredníctvom druhého dešifruje.

V praxi sa najčastejšie používa kombinácia symetrickej a asymetrickej kryptografie.



Komprimácia – kompresia

Komprimácia (kompresia, pakovanie či balenie) dát je proces, pri ktorom sa znižuje objem dát, pričom existujú dva druhy komprimácie:

- **nestratová** - pri ktorej nedochádza k strate údajov. To znamená, že ak skomprimované dáta dekomprimujeme, získame úplne identické dáta. Takto sa balia napríklad textové, programové a iné súbory. Kompresia sa deje na základe vynechania nadpočetných informácií. Kompresný pomer, ktorý predstavuje pomer medzi veľkosťou dát pred spakovaním a po ňom, sa tu dá dosiahnuť až okolo 2:1, niekedy aj viac, to však závisí od druhu dát.
- **stratová** - je proces, pri ktorom sa vynechajú tie údaje, ktoré sú pre celkový dojem z dát nepodstatné. Kompresný pomer je niekedy až 200:1, ale dáta sa už po kompresii nikdy nedajú zrekonštruovať do pôvodnej podoby. Časť informácií totiž chýba. Stratovú komprimácia používa hlavne pre komprimovanie mediálnych súborov a to zvuk, obraz, video ...

Komprimácia sa môže vykonávať:

- **automaticky** -uložením súboru v komprimovanom formáte JPG, MPEG, MP3
- pomocou špeciálneho **komprimačného programu** (ZIP, RAR).

Dekomprimácia sa deje buď samorozbalením alebo pomocou špeciálneho dekomprimačného programu. Niektoré dáta ostávajú trvale vo svojej komprimovanej podobe (najmä pri stratovej kompresii).